Se 2

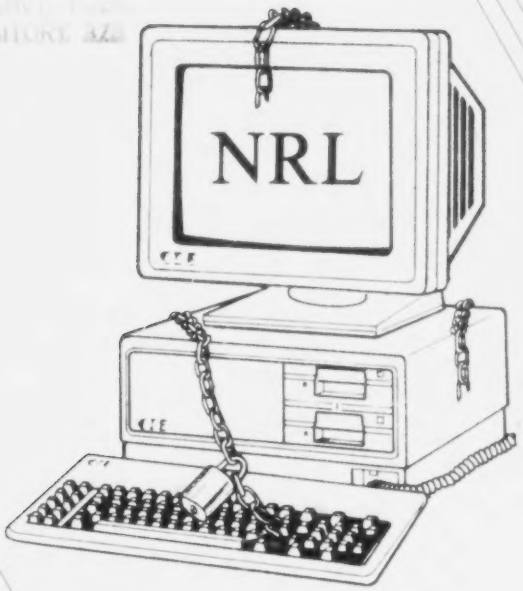
Naval Research Laboratory

Washington, DC
20375-5000

NRL Publication 0058-1200
January 1986

ADP SECURITY

at



D 210.2:

INTRODUCTION

Automatic data processing (ADP) has become a critical support system in today's research effort. If you depend on it, you must have confidence that your system will do what it should and nothing else. This is achieved by implementing a sound ADP security program.

This brochure highlights the need to include ADP security in the management and operation of each ADP system at NRL and provides an overview of how ADP security is achieved through the process of accreditation.

The degree to which an ADP system is secure depends on involvement by the personnel who manage and operate the system. Make an extra effort to ensure that your ADP system is operated in a secure fashion. Refer questions concerning ADP security to the NRL ADP Security Officer, Code 1220.1, 767-2240.

READEX FICHE best copy available

WHAT IS ADP SECURITY?

ADP security includes all of the measures which ensure that the ADP system does what it should and only what it should, when it should. It is the protection of the entire ADP resource including equipment, programs, data, facilities, people, and power.

WHY SHOULD I BE CONCERNED WITH ADP SECURITY?

People and machines are now in direct partnership. They form an effective and productive information system which involves certain risks which must be recognized and controlled. The purpose of ADP security is to provide a reasonable level of assurance that your ADP system does only what you want it to and that the data and programs which make up the system are reliable.

WHAT IS THE THREAT TO MY ADP SYSTEM?

Current news stories focus on the "hacker" threat. Deliberate attacks are real and when the ADP system is used to process classified data, the threat from hostile intelligence collectors is also real. When proprietary and administrative data are processed, protection from industrial espionage is a consideration. The primary threat from within the organization involves theft of ADP time or theft or misuse of hardware, data, or software.

HOW DO I SECURE MY ADP SYSTEM?

Generally speaking, effective security depends as much on positive attitude and management involvement as on technical safeguards. The security of an ADP system is inextricably bound to its overall management. No amount of superimposed security will make a poorly managed system safe. Although there is a growing tendency to look to exotic solutions to satisfy ADP security requirements, what is really needed in most cases is the application of sound management.

An effective ADP security program generally includes a combination of measures for protection, prevention and detection. The security measures which are required to protect a particular system are collectively identified and implemented through a process called ACCREDITATION.

WHAT IS ACCREDITATION?

Accreditation is a determination by the appropriate authority, designated in the Navy ADP Security Instruction, that, given the security measures in place, a system is operating at an acceptable level of risk. Every ADP system, including personal computers and word processors, must be accredited.

HOW DO I ACCREDIT MY SYSTEM?

To accredit your system, provide information about the ADP system to the NRL ADP Security Officer for analysis and endorsement. If the NRL ADP Security Officer identifies problems, he will work with you to correct them. The following may be required to accredit an ADP system, depending on its complexity and what kind of data is processed:

- a description of the system, its location and the amount and level of data processed;
- a risk assessment — an assessment of the threats to the system, how likely they are to occur and their impact on the system;
- a security test and evaluation — an analysis of the effectiveness of the security measures which protect the system;
- a contingency plan — documented plans to minimize the impact of an occurrence which affects the operation of the ADP system, measures and plans to recover from the occurrence and plans to continue operating while recovery is taking place; and
- documented system security procedures — written security policies and procedures for operating the system.

WHAT MEASURES SHOULD I USE TO PROTECT MY ADP SYSTEM?

A requirement for requesting accreditation is an analysis of the threats to the system and identification of security measures to counter those threats. Security measures which are commonly used to protect ADP systems include:

- cypher locks, combination locks, alarms and other physical security devices;
- fire alarm and extinguishing systems to protect the system from the threat of fire;
- review of audit records which show system access and exceptions to normal system activity;
- passwords and special procedures to control access to the information and programs in the system;
- use of encryption to protect the data communicated between the ADP system and remote devices; and
- secure off-site storage of duplicate copies of data and programs to minimize damage in case of a disaster.

WHO IS RESPONSIBLE FOR PROVIDING SECURITY FOR AN ADP SYSTEM?

The cognizant division director is ultimately responsible for the security of an ADP system, and appoints someone to be responsible for planning and implementing security for the system. This person is called the ADP System Security Officer (ADPSSO).

DOES NRL HAVE A COMMAND SECURITY POLICY?

Yes. The NRL Command ADP security policy is that ADP security is the responsibility of everyone involved with managing, using, operating and maintaining an ADP system. Each employee is required to adhere to ADP security policies and to report violations. ADP resources may be used only for official purposes. Fraud, waste, abuse, and misuse of ADP resources are serious matters and may result in disciplinary or legal action being taken against the offender.

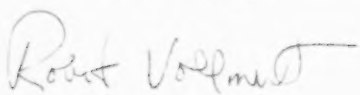
WHAT SHOULD I DO IF I DISCOVER A SECURITY VIOLATION?

Any significant security violation should be reported immediately to the ADP Security Officer (Code 1220.1). Anyone suspected of complicity in the violation should be denied access to the computer and all of its associated resources until the violation can be investigated.

SO, WHAT DO I DO NOW?

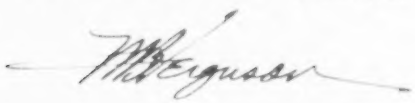
The best thing to do is to get involved in planning security for your ADP system. Become part of the solution. Find out whether your system is accredited. If not, take action to accredit it. If you have questions about ADP security, contact your Division ADP Security Representative or the NRL ADP Security Officer.

PREPARED BY:



R.G. VOLLMERT, CODE 1220.1

REVIEWED AND APPROVED: 1/86



(Reviewing Officer)